

(19)日本国特許庁 (JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開平9-198437

(43)公開日 平成9年(1997)7月31日

(51)Int.Cl. <sup>6</sup>	識別記号	序内整理番号	F I	技術表示箇所
G 0 6 F 17/60			G 0 6 F 15/21	Z
	19/00	7259-5 J	G 0 9 C 1/00	6 3 0 Z
G 0 9 C 1/00	6 3 0	7259-5 J		6 4 0 D
	6 4 0	7259-5 J		6 6 0 D
	6 6 0	7259-5 J		6 6 0 E

審査請求 未請求 請求項の数2 O L (全6頁) 最終頁に続く

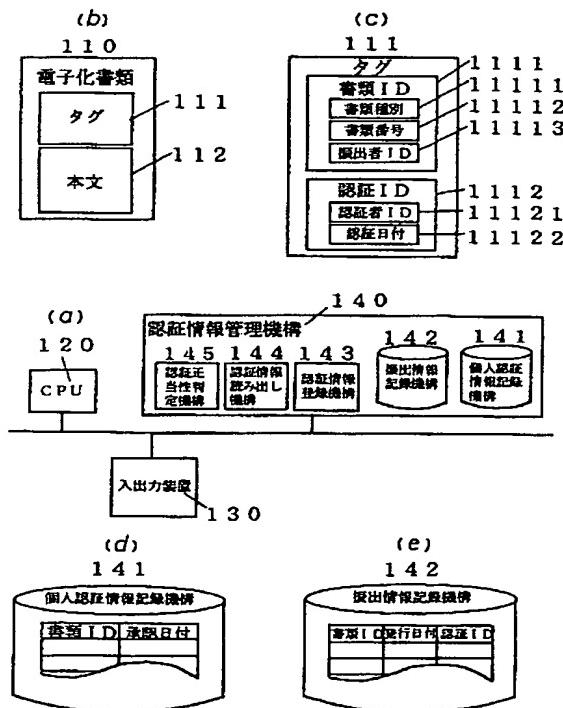
(21)出願番号	特願平8-6361	(71)出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目6番地
(22)出願日	平成8年(1996)1月18日	(72)発明者	葛西 健人 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内
		(72)発明者	松下 博則 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア開発本部内
		(72)発明者	村上 昌彦 神奈川県秦野市堀山下1番地 日立コンピュータエンジニアリング株式会社内
		(74)代理人	弁理士 磯村 雅俊

### (54)【発明の名称】電子認証の管理方法

#### (57)【要約】

【課題】電子認証において、書類の発行記録・発行した書類の記録・認証記録・最終処理の記録等の認証情報を、電子化書類と認証者の電子計算機の両方に記録し、電子化書類に付随する認証情報と、認証者の個々の電子計算機内の認証情報との整合性の確認によって、書類の発行・認証の途中経過・最終状態等の認証の正当性の判定を実施することで、認証情報の改竄の発見を容易とし、認証情報の改竄を困難とする。

【解決手段】認証情報は、電子化書類110のタグ111に記録された認証情報と、認証者の電子計算機の個人認証情報記録機構141に記録された認証情報とに、分散し多重化されている。電子化書類110のタグ111の認証情報を改竄しても、電子化書類110のタグ111の認証情報と認証者の電子計算機の個人認証情報記録機構141に記録された認証情報を、認証正当性判定機構145が整合性を確認することで簡単に改竄が発見できる。



## 【特許請求の範囲】

【請求項1】 認証者が電子計算機にて電子化書類の認証を行う方法において、

電子化書類の認証情報を当該電子化書類に付随させるとともに認証者の電子計算機に記録し、

電子化書類に付隨する認証情報と認証者の電子計算機内の認証情報との整合性の確認によって、当該電子化書類の認証の正当性を判定することを特徴とする、電子認証の管理方法。

【請求項2】 認証者が電子計算機にて電子化書類の認証を行う方法において、

電子化書類の認証情報を当該電子化書類に付隨させるとともに認証者の電子計算機に記録し、当該認証情報を定期的にバックアップ用の補助記録手段に複写し、

電子化書類に付隨する認証情報と認証者の電子計算機内の認証情報との整合性の確認によるか、電子化書類に付隨する認証情報と前記補助記録手段の認証情報との整合性の確認によって、当該電子化書類の認証の正当性を判定することを特徴とする、電子認証の管理方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、電子化書類における電子認証の管理方法において、認証情報を電子化書類と認証者の電子計算機の両方に記録することで、認証記録の改竄を困難にする方法に関する。

## 【0002】

## 【従来の技術】

(1) 従来の、電子化書類の認証の管理は、認証の印として認証者固有の印影を認証情報として記録し、これを確認する方式がある。この場合、印影の正当性は、印影使用の正当性で保証される。

(2) 従来の、電子化書類の認証の管理は、認証の印としてユーザIDを認証情報として記録し、これを確認する方法がある。この場合、ユーザIDの正当性は、ユーザIDの使用の正当性で保証される。

(3) 従来の、電子化書類の認証の管理は、電子化書類を暗号化し、鍵の設定により認証可能な認証者をを特定することで、これを確認する方式がある。この場合、認証の正当性は、鍵の使用の正当性によって保証される。

なお、(1)特開平02-278937号公報には、電子化書類の承認・不承認・修正の履歴をとることで、再承認作業の効率化に関する技術が記載されている。また、(2)特開平05-290066号公報には、認証の印として電子化された画像による印影を用いる方式に関する記載がある。また、(3)特開平06-119363号公報には、電子化書類の更新権限の設定をパスワードで行う方式に関する記載がある。

## 【0003】

【発明が解決しようとする課題】上記従来技術(1)は、印影使用の正当性が認証者の印影の管理に委ねられ

ており、また、電子化された印影は複写が容易であることから、印影の盗用による認証記録の改竄が可能という問題があった。上記従来技術(2)は、ユーザIDおよびパスワードの正当性が認証者の管理に委ねられており、また、ユーザIDおよびパスワードは簡単な英数字列であることが多いため、ユーザIDおよびパスワードの盗用による認証記録の改竄が可能という問題があった。上記従来技術(3)は、鍵の正当性が認証者の管理に委ねられており、また、鍵は簡単な英数字列であることが多いため、鍵の盗用による認証記録の改竄が可能という問題点があった。本発明の目的は、このような問題点を改善し、認証情報の改竄の発見を容易とし、認証情報の改竄を困難とすることが可能な電子認証の管理方法を提供することにある。

## 【0004】

【課題を解決するための手段】上記目的を達成するために、本発明は、分散・多重化された認証情報により電子認証を行う。すなわち、電子化書類に付隨して記録された認証情報（例えば、書類の発行記録・発行した書類の記録・認証記録・最終処理の記録・書類に関係するその他の記録の認証情報）と、認証者の電子計算機に記録された認証情報またはバックアップ用の補助記録手段に複写記録された認証情報との整合性を確認することによって、書類の発行・認証の途中経過・最終状態等の認証の正当性の判定を実施する。

## 【0005】

【発明の実施の形態】本発明においては、認証情報は、電子化書類に付隨して記録された認証情報と、それぞれの認証者の電子計算機あるいはバックアップ用の補助記憶手段に記録された認証情報とに、分散し多重化されている。それによって、電子化書類に付隨した認証情報を改竄しても、認証者の電子計算機あるいはバックアップ用の補助記憶手段に記録された認証情報との整合性を確認することで、簡単に改竄が発見できる。なお認証情報の改竄には、承認・不承認の変更、認証対象者の変更がある。

【0006】以下、本発明の実施例の詳細を図面に基づいて説明する。図1は、本発明の一実施例の装置構成を示す図である。同図において、110は電子化書類、111はタグ、112は本文、120は装置全体を統括制御するCPU、130は装置へ及び装置からの入出力装置、140は認証情報管理機構、141は個人認証情報記録機構、142は振出し情報記録機構、143は認証情報登録機構、144は認証情報読み出し機構、145は認証正当性判定機構である。本実施例の電子計算機システムは、(a)に示す通りであって、電子化書類110は、(b)に示すように、タグ111と本文112から構成される。タグ111は、(c)に示すように、電子化書類に付隨する認証情報で、書類を特定する書類ID1111および認証の対象者・認証の状態を示す認証

ID1112から構成され、書類の認証情報を記録する。書類を特定する書類IDには、書類の重要度や緊急度を示す書類種別11111、当該書類が一意であることを示す書類番号11112、振出者ID11113から構成される。発行の記録には、発行の事実および日付時間がある。認証の対象者には、氏名およびユーザIDがある。認証の状態を示す認証ID1112には、認証者を特定する認証者ID11121・認証日付11122から構成される。認証情報管理機構140は、個人認証情報記録機構141、振出情報記録機構142、認証情報登録機構143、認証情報読み出し機構144、認証正当性判定機構145から構成される。認証情報登録機構143は、電子化書類110が作成されると、そのタグ111および本文112に基づいて、振り出し記録を、(e)に示す振出情報記録機構142に登録する。振り出し記録には、書類ID1111・発行日付および認証対象者を特定する認証ID1112を記録する。また、電子化書類110について認証が実施されると、その認証情報を個人認証情報記録機構141に登録する。個人認証情報記録機構141は、(d)に示すように、認証者の電子計算機における認証者個人の認証情報記録機構で、書類ID1111・認証日付11122を記録する。認証情報読み出し機構144は、認証正当性判定機構145の要求に基づいて、個人認証情報記録機構141から当該電子化書類110の認証情報を取り出し、当該認証正当性判定機構145に返す。認証正当性判定機構145は、当該電子化書類110のタグ111の認証情報に基づいて、当該電子化書類110の認証確認対象者を選定し、自動的または操作者の指示に基づいて、一部または全ての認証確認対象者の電子計算機の認証情報読み出し機構144に対して認証情報の提示を要求し、各認証情報読み出し機構144から返された認証情報と当該電子化書類110のタグ111の認証情報との整合性を確認し、認証記録の正当性を判定する。

【0007】図2は、本発明の一実施例の電子化書類の認証と認証の確認の流れを簡単に示す図である。同図において、振り出し者210の電子計算機で電子化書類220が作成されると、電子化書類の振り出し情報が、振り出し者210の電子計算機の振出情報記録機構211と電子化書類220のタグ221に記録され、最初の認証対象者230の電子計算機に向けて電子化書類220が振り出される。電子化書類220が最初の認証対象者230の電子計算機に到達し認証された場合、その認証情報が、認証対象者230の電子計算機の個人認証情報記録機構231と電子化書類220のタグ221に記録され、電子化書類220が次の認証対象者240に回覧される。電子化書類220が最終判断者250の電子計算機に到達した場合、最終判断者250は当該書類のタグ221に記録された書類ID2211の書類種別で示される書類の重要度や緊急度に応じて認証の確認が必要

か判断する。認証の確認が必要であると判断した場合、最終判断者250は最終判断者250の電子計算機から認証正当性の確認を行う。

- 【0008】図3は最終判断者310の認証正当性確認処理の流れを示す図である。同図において最終判断者310は、最終判断者310の電子計算機の認証正当性判定機構311に対して認証確認対象者を指定して、電子化書類320の認証の正当性の確認を指示する。最終判断者310の電子計算機の認証正当性判定機構311は、最終判断者310の指示に基づいて認証確認対象者330の電子計算機の認証正当性判定機構331に、当該書類320の書類ID321を送信し、認証確認対象者330が、当該書類320を正当に認証しているか否かを問い合わせる。書類ID321を受け取った認証確認対象者330の電子計算機は、当該電子計算機の認証正当性判定機構331から認証情報読み出し機構332に対し、当該書類ID321が示す書類320の認証情報の読み出し指示を出す。認証情報読み出し機構332は、個人認証情報記録機構333から当該書類320の認証情報の読み出し処理を行い、当該書類320の認証情報が個人認証情報記録機構333に登録されていた場合、認証正当性判定機構331に読み出した認証情報を返す。また、当該書類320の認証情報が個人認証情報記録機構333に登録されていなかった場合、認証正当性判定機構331に当該書類ID321が示す書類320の認証情報無しのメッセージを返す。認証確認対象者330の認証正当性判定機構331は、個人認証情報記録機構333から返された読み出し結果が、最終判断者310から受信した書類ID321で示す書類320が承認されているという場合、認証情報の承認のメッセージ334を最終判断者310の電子計算機に応答する。また、当該書類ID321無しの場合、または当該書類320は不承認であるという認証情報の場合、不承認のメッセージ334を最終判断者310の電子計算機に応答する。次に、メッセージ334を受けた最終判断者310の電子計算機は、ディスプレイ装置または他の出力装置により、認証確認対象者330の承認および不承認の情報を最終判断者310に提示する。最終判断者310は、提示された承認および不承認のメッセージに基づき、当該書類320に対する認証の正当性を確認、決裁の判定を行う。また、本認証の確認は最終判断者以外の認証者が、その時点での認証の正当性の判定に用いることも可能である。
- 【0009】なお、本実施例では、個人認証情報記録機構に認証情報を記録しているが、この他にバックアップ用の補助記録装置を設けてもよい。あるいはその補助記録装置をデータベース化してもよい。これにより、当該認証者の電子計算機がダウンしている場合でも電子化書類の認証の正当性を判定することができる。また、最終判断者の認証判定は、電子計算機が自動的に行うように

してもあるいは操作者の指示により行うようにしてもよい。

#### 【0010】

**【発明の効果】**本発明によれば、電子認証の確認方法として、ID、パスワード、鍵といった単一または複数の秘密の正当性を判定する方式に比べ、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認する方式は、改竄においては電子化書類と認証者全員の電子計算機の認証情報が対象となり、その冗長性において認証情報の改竄を困難とするとともに、改竄の発見を容易とする。また、電子認証の確認方法として、ID、パスワード、鍵といった単一または複数の秘密の正当性を判定する方式に比べ、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認する方式は、盗用される秘密が存在せず、秘密の盗用による改竄は不可能である。また、電子化書類と認証者の電子計算機に分散し多重化された認証情報の整合性を確認するため、特別な暗号・復合のための機構が不要である。

#### 【図面の簡単な説明】

【図1】本発明の一実施例における電子計算機システムの装置構成を示す図である。

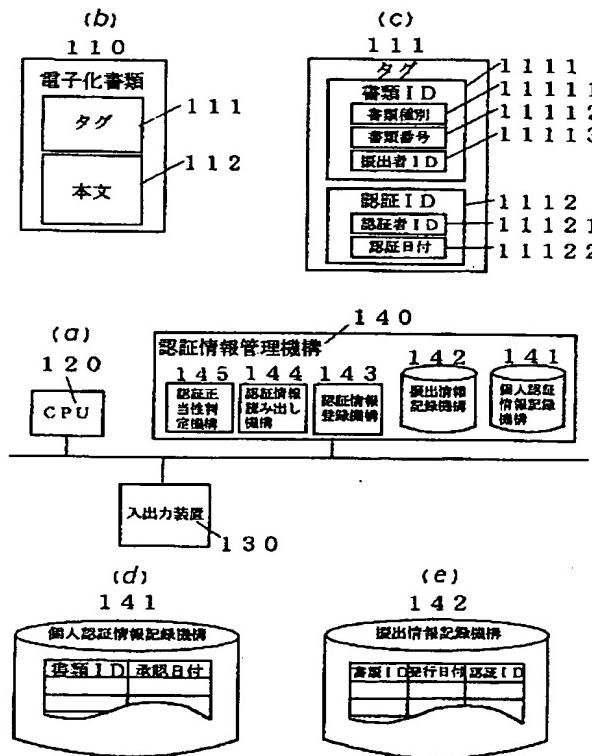
【図2】本発明の一実施例の電子化書類の認証と認証の確認の流れを簡単に示す図である。

【図3】本発明の一実施例の最終判断者の認証正当性確認処理の流れを簡単に示す図である。

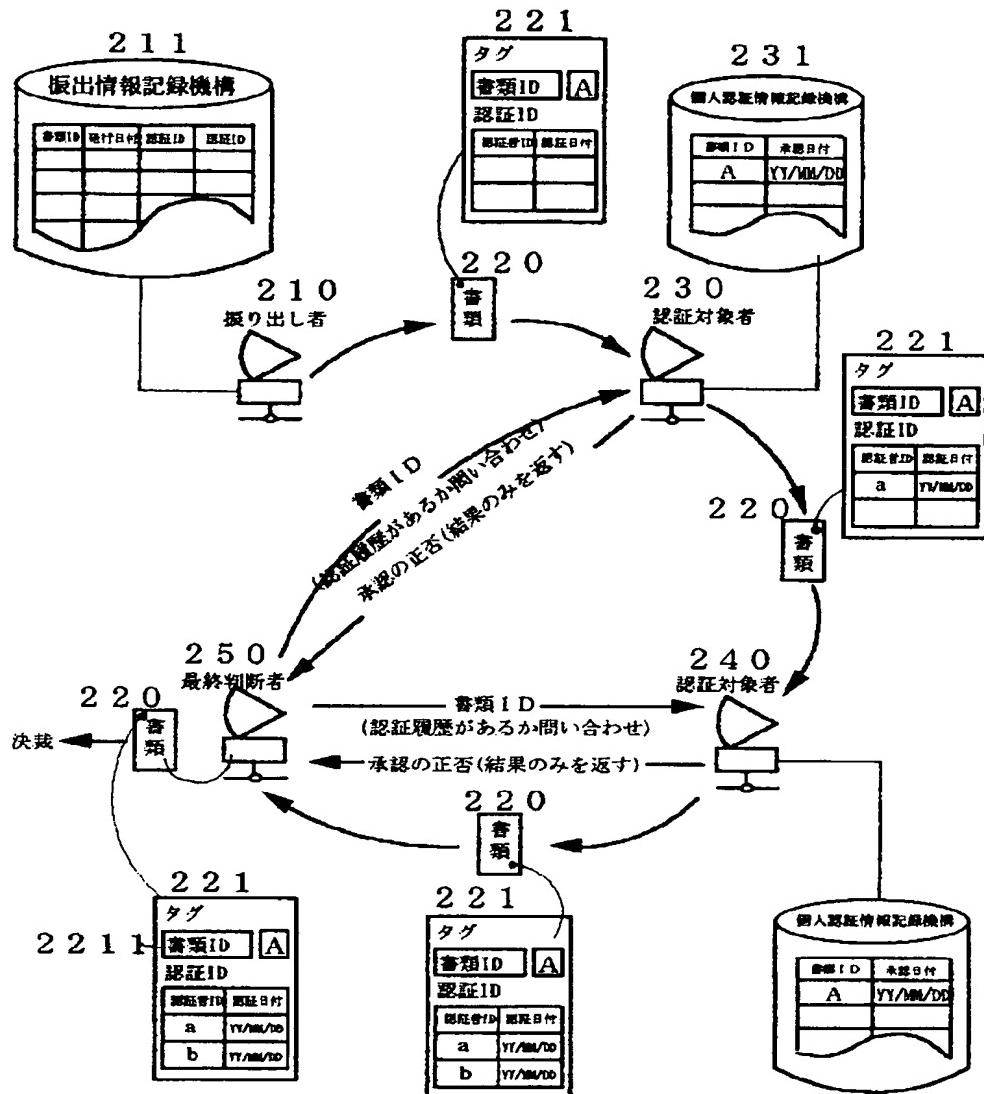
#### 【符号の説明】

110：電子化書類、111：タグ、1111：書類ID  
 D、11111：書類種別、11112：書類番号、11113：振出者ID、11112：認証ID、111121：認証者ID、111122：認証日付、112：本文、12：CPU、130：入出力装置、140：認証情報管理機構、141：個人認証情報記録機構、142：認証情報登録機構、143：認証情報読み出し機構、144：認証正当性判定機構、145：認証情報読み出し機構、210：振出し者、211：振出情報記録機構、220：電子化書類、221：タグ、2211：書類ID、230：認証確認対象者、231：個人認証情報記録機構、240：認証確認対象者、250：最終判断者、310：最終判断者、311：認証正当性判定機構、320：電子化書類、321：書類ID、330：認証確認対象者、331：認証正当性判定機構、332：認証情報読み出し機構、333：個人認証情報記録機構、334：メッセージ（承認・不承認）。

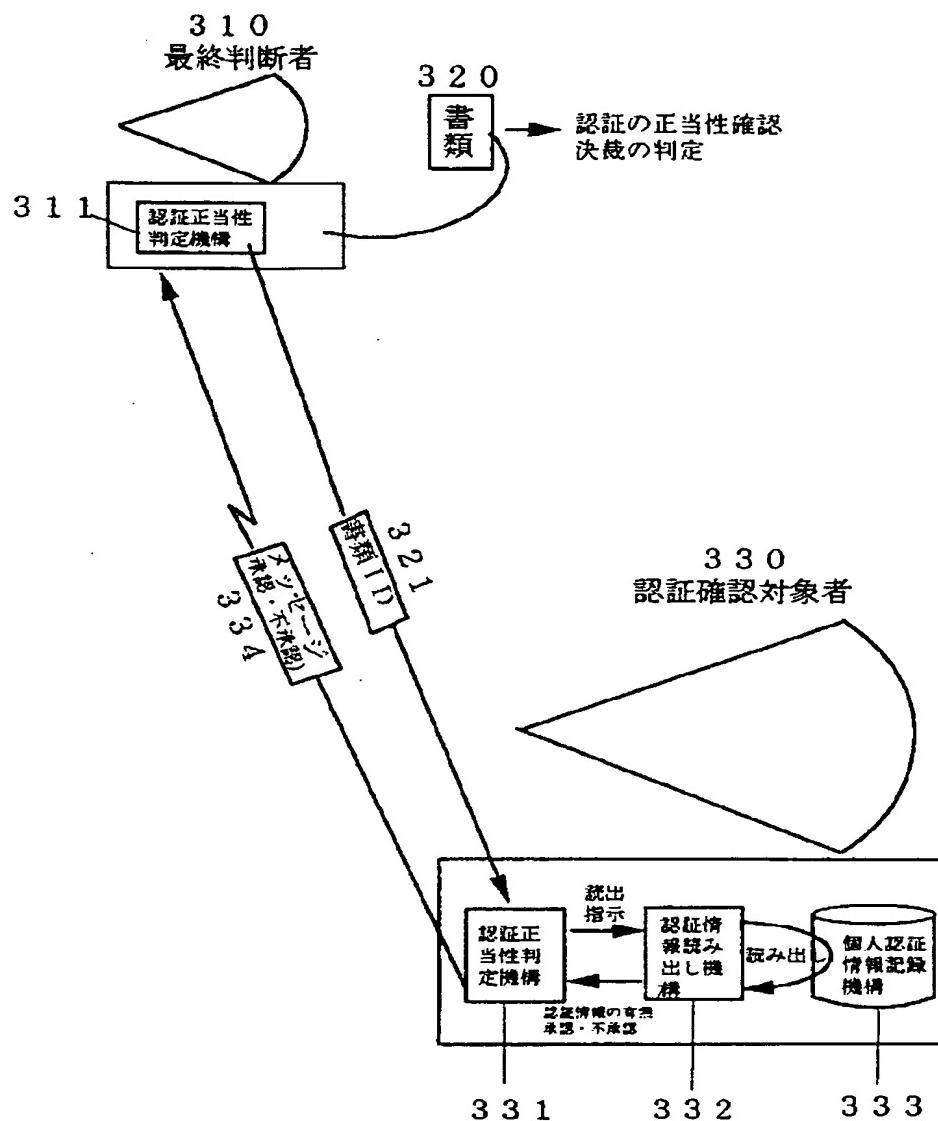
【図1】



【図2】



【図3】



フロントページの続き

(51) Int. Cl. <sup>6</sup>	識別記号	府内整理番号	F I	技術表示箇所
G 0 9 C	1/00	6 6 0	G 0 6 F 15/22	Z
H 0 4 L	9/32		15/30	H
			H 0 4 L 9/00	6 7 3 Z